PURESTORAGE®
Uncomplicate Data Storage, Forever

TECHNICAL WHITE PAPER

Ransomware Mitigation with Pure Storage and Commvault

Best practices for Object SafeMode with
Pure Storage FlashBlade//S and Commvault.

Contents

Introduction

Ransomware is one of the biggest threats to businesses today, and it's not showing any signs of slowing down. Attacks are constantly getting more sophisticated. Ransomware groups are identifying and exploiting new vulnerabilities before manufacturers can patch them. Security Brief Australia reports that "52% of widespread threats began with a zero-day exploit." Ransomware-as-a-service groups have been on the rise for several years, making it much easier for attackers to exploit these new vulnerabilities. That's a big part of why Cybersecurity Ventures predicts ransomware to cost companies more than $250 billion worldwide by 2031.

And attacks can be incredibly expensive. According to a Statista study, while the average disruption from a ransomware attack decreased over 2021—from 23 days to 20—it is still up 33% compared to 15 days in Q1 2020. Sophos' State of Ransomware 2022 calculated that the average cost of remediating a ransomware attack was $1.4 million. That means if you're down due to an attack, the recovery, lost revenue, and reputational loss could cost as much as a full-time IT employee's annual salary, every 2 days or less.

Minimizing the impact of an attack is critical to keeping the cost down. Rapid Restore with Pure FlashBlade//S® and Commvault significantly reduces how much time you need to spend on recovery. Object SafeMode™ keeps an attacker from destroying days' worth of data or your ability to recover. And with insurance companies raising premiums and increasing requirements for cyber coverage, ensuring recoverability and being able to restore your systems quickly are important for helping you secure a policy with a lower price.

This white paper is intended as a how-to and best practices guide to assist with the design and implementation of Pure Storage® FlashBlade//S™ Object SafeMode™ into Commvault environments. The best practices apply only to configuration elements specific to Object SafeMode and not necessarily to general FlashBlade//S deployments. For general best practices for using FlashBlade//S with Commvault, contact your Pure Storage account team. For Commvault best practices around ransomware protection, please see Commvault's own documentation.

The target audience for this document includes, but is not limited to, system architects, systems engineers, IT managers, and storage administrators. This guidance applies equally to FlashBlade//S and first-generation FlashBlade®, except as noted.

Augment Data Protection with Object SafeMode

At Pure Storage, we share your concerns around ransomware. Object SafeMode, a built-in feature of FlashBlade//S systems, mitigates these attacks by preventing any modification or deletion of backup data. Because the backup data can't be altered or destroyed, it's available immediately, helping guard against attacks by ransomware, accidental deletion, and even rogue admins. SafeMode™, another built-in FlashBlade//S feature, further enhances protection by capturing Commvault's master databases in periodic read-only snapshots.

FlashBlade//S provides the following benefits:

- **Enhanced protection**: Ransomware can't delete, modify, or encrypt data protected with Object SafeMode. In addition, only an authorized designee from your organization can work directly with Pure Technical Support to configure the feature, modify policy, or manually eradicate data.
- **System-wide security**: Once enabled, Object SafeMode protects all object buckets on the FlashBlade//S, not just ones used by Commvault.
- **Backup integration**: Object SafeMode and SafeMode snapshots are transparent to Commvault.
- **Flexibility**: The object immutability period is customizable up to 400 days.
- **Rapid restore**: Leverage a massively parallel architecture and elastic performance that scales with data to speed backup and, moreover, recovery.
- **Investment protection**: FlashBlade//S includes Object SafeMode at no extra charge. Your Pure subscription or maintenance support contract covers enhancements.

Pure Storage FlashBlade//S

Pure Storage FlashBlade//S is the next generation of enterprise scale-out unified fast file and object (UFFO) storage that delivers rich data services with high density, capacity, performance, and scalability to meet the needs of modern applications. Using a distributed metadata architecture, FlashBlade//S offers multi-dimensional performance on a consolidated platform with NFS, SMB, and S3 protocol access.

Modular Architecture

FlashBlade//S has a unique modular architecture that enables organizations to unlock new levels of power, space, and performance efficiency using an all-QLC design. The architecture disaggregates compute resources from storage so that capacity and compute can scale independently for extreme flexibility in configuration. FlashBlade//S (Figure 1) is a customizable platform that gives you the ability to tailor your configuration for current workload requirements and to non-disruptively upgrade to meet future needs. You can upgrade components on a schedule that is consistent with changing technologies to future proof the system.

Figure 1. FlashBlade//S

Chassis

The FlashBlade//S chassis is 5RU high and has bays for mounting ten blades. Fully populated with high-density blades, a chassis holds 1.92PB of physical flash with headroom for future density increases.

The chassis midplane distributes power and has dual Ethernet links capable of operating at 100Gbps to each blade. Blades connect to two Fabric I/O Modules (FIOMs) on the midplane. The FIOMs have Ethernet switches that connect blades to the client network, or in multi-chassis systems, to external Fabric Modules (XFMs).

The chassis has four power supply units (PSUs), each rated at 2,400 watts. The PSUs are "2+2 redundant"—any two of them can supply the chassis' maximum rated power of 4,800 watts, to accommodate the greater demands of future components.

Blade

The blades have CPUs, NICs, DRAM, and four DirectFlash® module (DFM) mounting slots. Blades use NVMe over on-board PCIe to communicate with their DFMs. You can configure blades with either performance-optimized (24TB) or capacity-optimized (48TB) DFMs.

Blades operate with one, two, three, or four DFMs installed. All blades in the chassis must have the same number of DFMs in each blade. Systems can be configured for applications from the very read-intensive (e.g., artificial intelligence and machine learning) to those requiring extremely high capacity (e.g., backup and archiving).

The blade design isolates failure domains. You can replace a failed DFM from the front of the chassis without affecting its blade's ability to function. DFMs can move to different bays in a chassis to minimize the operational impact of recovering from blade failures or replacements.

DFMs with QLC Flash

Architectures that use off-the-shelf solid-state drives (SSDs) have an internal controller to manage the flash media on each specific drive. These systems do not have any visibility into what is happening at the system level. FlashBlade//S takes a different and innovative approach with DirectFlash Modules (DFMs) that enable the storage operating system to manage the media on a global level. Global media management unlocks as much as 20% more capacity from NAND compared to systems that use off-the-shelf SSDs, and delivers more consistent performance, better reliability, and higher media endurance without the need for a massive and expensive storage class memory (SCM) cache.

Network Fabric

The integrated networking in FlashBlade//S simplifies large-scale deployments by collapsing three networks (front-end, control, and back-end) into one high-performance software-defined networking (SDN) fabric. This SDN is shared across the two fabric modules in the platform, and it hides the complexity of networking from the administrator.

FlashBlade//S virtualizes the network so that no matter the size of the platform, it appears as one entity. This virtualization simplifies load balancing and cabling. Each blade can service and restart any client connection and run any protocol, and the platform is stateless because the logic can run anywhere.

Dual Fabric I/O Modules (FIOMs) interconnect blades, connect chassis (in multi-chassis systems), and connect blades to clients. The FIOMs have ethernet switches with eight (8) external ports each capable of 10, 25, 40, or 100Gbps transmission rates. The switches have a total of 2Tbps cross-sectional bandwidth. Each FIOM uses 50Gbps for inter-blade communication in the chassis. Both FIOM switches and blade NICs are capable of 100Gb/s for future expansion.

Purity//FB

The Purity//FB operating system is the heart of FlashBlade//S, enabling scalability in capacity and performance. Purity//FB is all-inclusive software with enterprise-grade data services. The design of Purity//FB optimizes the power of the hardware with its variable block metadata engine and scale-out metadata architecture. It can manage billions of files and objects and deliver unmatched performance for any workload, whether it's sequential or random access with large or small files and objects. Purity//FB delivers a rich set of enterprise capabilities including compression, global erasure coding, always-on encryption, SafeMode™, file replication, object replication, and multiple other features.

Environmental Efficiency

Today, more than ever, environmental, social, and corporate governance (ESG) initiatives are becoming more important. As a result, space and power constraints are now becoming crucial considerations in storage strategy. The architectural design of FlashBlade//S uncomplicates the relationship between data storage and a lower carbon footprint. It is designed to save data center space with streamlined energy consumption and more efficient power and cooling. When combined, this creates a storage solution that has a significant and immediate impact on the environment while lowering overall TCO.

FlashBlade//S and Evergreen//Forever

The modular design of FlashBlade//S simplifies adding storage capacity and compute resources with non-disruptive hardware upgrades. This has made it possible for Pure to offer Evergreen//Forever™ service for the new systems. Evergreen//Forever has several advantages, including the Forever Flash lifetime media guarantee, Ever Agile upgrades with trade-in credits, "flat and fair" service pricing guarantees, and periodic hardware refresh at no incremental cost.

New generations of storage hardware typically appear every three to five years. Historically, this meant that every three to five years users would effectively repurchase capacity they already owned and must migrate hundreds of terabytes of data from old to new hardware. Evergreen//Forever plus the non-disruptive upgrades on FlashBlade//S enable the system to keep pace with hardware evolution. FlashBlade//S gets better over time.

Recommended Architecture

The Pure Storage best practice for deploying FlashBlade//S with Commvault is to use object storage, accessed over Amazon S3 protocol, for the primary data copy for performance and simplicity. Object SafeMode adds object-level immutability without any changes to the logical architecture.

CommServe DR backups can benefit from SafeMode Snapshot protection when using an SMB share on FlashBlade//S. For instructions on enabling SMB support on FlashBlade//S and connecting to Active Directory, please see FlashBlade//S documentation.

Figure 2 shows the reference architecture with both Object SafeMode protecting backups of primary data and SafeMode snapshots protecting CommServe DR backups.

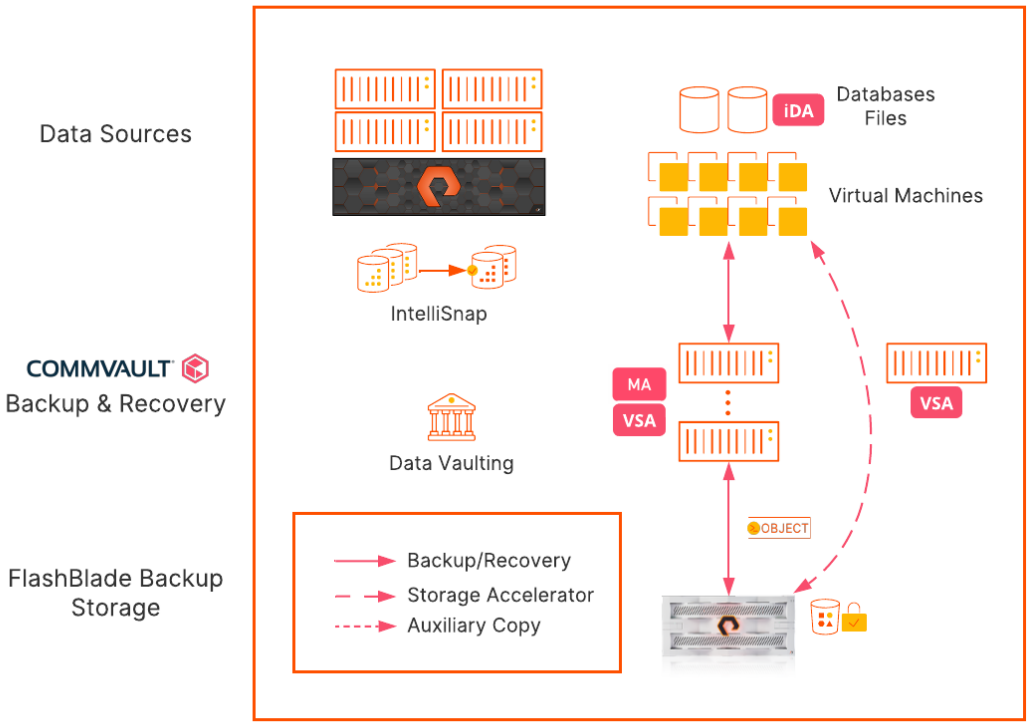

Figure 2. Recommended architecture

Immutability and Global Deduplication

While it's indisputably valuable for reducing storage consumption, global deduplication has major implications for implementing immutability at an object level. It's important to understand the impact to make the right design decisions. Virtually all backups will depend on data written by earlier backups. As an example, assume you need to ensure your backups are locked for seven days. Your backups for day six need to have all the previous days' data available too, because there will be references to some of it. In fact, the protection must extend all the way to the very first backup, otherwise someone could just wait until your oldest data is exposed, delete it, and destroy recovery from last night's backup. That's true regardless of how long you keep your backups, because even day 30 backups might depend on day one data. The bottom line is you would need to lock all your data forever to protect any of it, which would mean nothing could ever age. Figure 3 illustrates this dependency.

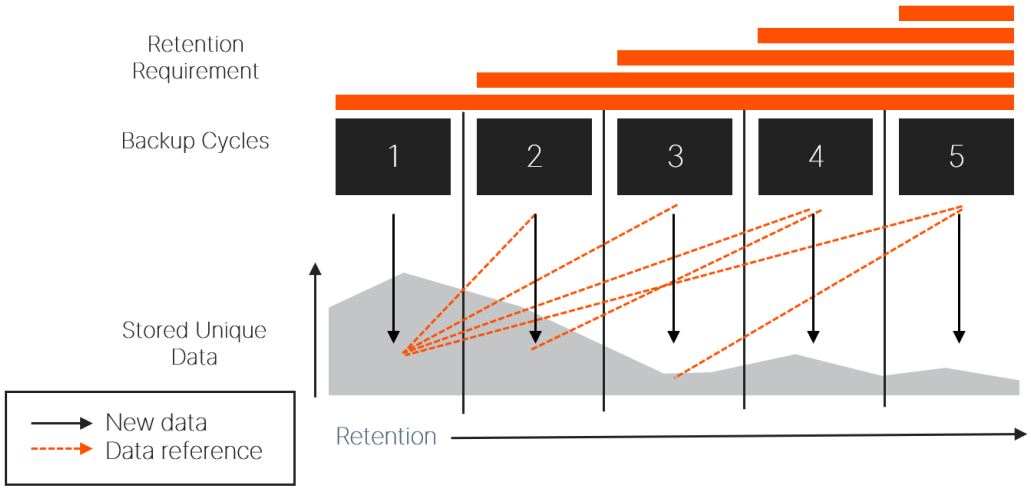

Figure 3. Deduplication dependencies

The solution is to use a layered data vaulting concept. Commvault periodically "closes" the vault against new data and starts a new one. FlashBlade//S Object SafeMode protects the vaulted data from external deletion or changes to ensure that the data dependencies remain intact until the last data in the vault expires. Commvault's data retention system deletes stale objects as Object SafeMode releases them.

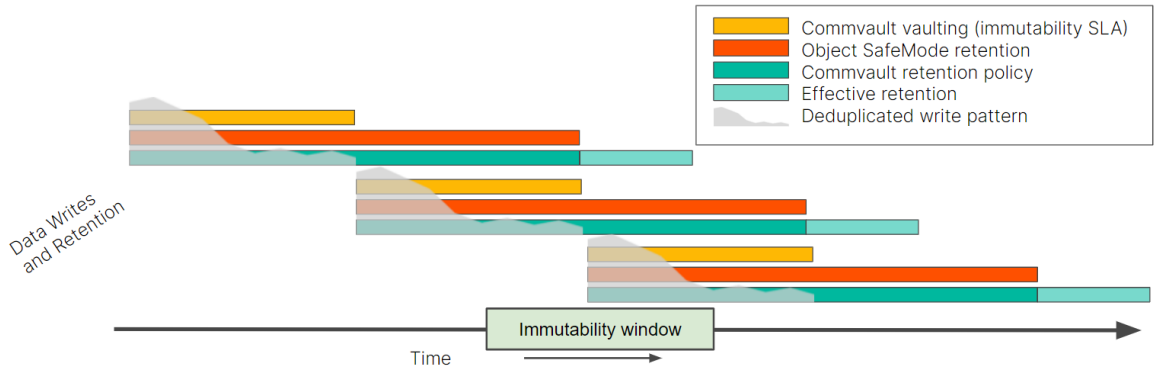

Figure 4. Layered data vaulting

The layered vaulting system protects your data from initial backup for the entire SLA period. It does not require any periodic point-in-time snapshots, and there is no gap between when data is written and when it's protected. You can start recovery from a ransomware attack without first having to recover your backup data, so your production systems will be online sooner.

Layered vaulting does require additional storage since each deduplication baseline will age after the next one is created, but it requires less storage than backup without deduplication.

Best Practices and Procedures

These best practices are organized to encapsulate the components of the architecture, from foundations to MediaAgent configuration, data copy, server plans, and DR backup. Each section covers the entire configuration of the component.

Foundations

Design Layered Vaulting Around Immutability SLA

When you are designing your layered vaulting approach, you should start with the immutability SLA, the length of time you need to guarantee your data is protected. While it is possible to work backward starting with your backup retention policies, it is easier to build layers up from the SLA.

> NOTE: As you plan for vaulting, remember that Object SafeMode is a system-level policy and will apply to all object data stored on the FlashBlade//S, not just Commvault data. If you need guidance or discussion on determining the right settings for your environment, please contact your Pure account team.

The Commvault vaulting interval should match your SLA. Aligning to a multiple of seven days will give the easiest calculations for the other layers.

The Object SafeMode retention period should be double the Commvault vaulting interval to ensure each entire vault meets the SLA. For example, for a seven-day vaulting interval, Object SafeMode needs to have a 14-day retention period to protect the data from day seven for seven days. An authorized company contact will work with Pure Storage Support to configure the Object SafeMode retention period.

The Commvault retention policy should be set to match Object SafeMode. For example, if Object SafeMode retention is set for 14 days, Commvault retention should also be set to 14 days. While it can be longer or shorter depending on your specific needs, the storage calculations are simpler when you align to backup cycles. Setting the Commvault retention policy to less than the Object SafeMode retention period will not save any storage since data will still be locked after it ages within Commvault software. A longer retention policy will require more storage.

Figure 5 shows the relationship between the vault layers and the formulas for each layer.

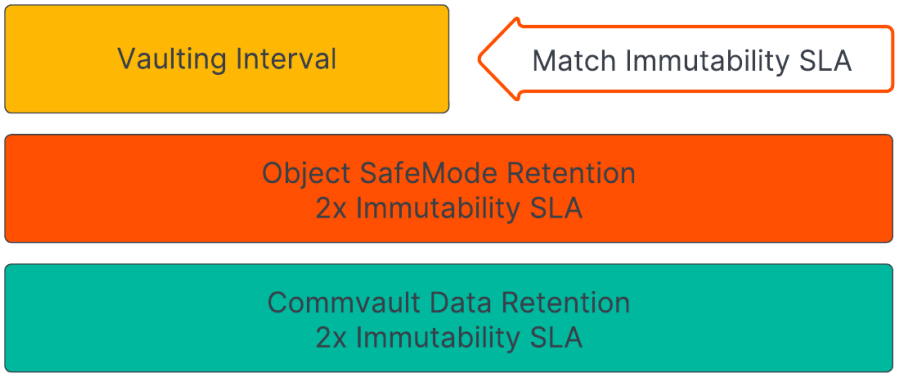

Figure 5. Vault layer relationships and formulas

Table 1 shows the recommended settings for several example scenarios. You should contact your Commvault or Pure account team if you have questions or want to discuss more complex retention needs.

Immutability SLA	Commvault Data Vault	Object SafeMode Retention	Commvault Retention Policy
7 days	7 days	14 days	14 days
14 days	14 days	28 days	28 days
21 days	21 days	42 days	42 days

Table 1. Layered data vaulting formulas and examples

Use Purity//FB 3.3.3 or Later

Purity//FB 3.3 introduced the ability to enable Object SafeMode with existing object buckets. Release 3.3.3 includes several important fixes and is the minimum recommended version for first-generation FlashBlade arrays. FlashBlade//S supports only Purity//FB release 4.0 and later.

Use Commvault Release 2022E or Later

While Object SafeMode is compatible with all Commvault releases 11.20 and newer, 2022E, also referred to as 11.28, is the most recent long-term support release as of this writing. Along with general improvements, 2022E includes enhancements that make the solution simpler to deploy and manage.

Schedule Full Backups at Least Weekly

You should schedule full or synthetic full backups at least weekly for all data protected with Object SafeMode. Since data aging is closely tied to full and synthetic full backups, longer backup cycles will take longer to release older data, consuming more storage.

Estimate Capacity Requirements

In a Commvault environment, implementing Object SafeMode will require capacity to store the data vaults until they expire. For most environments you will need about twice the amount of data you plan to protect at the end of the projection period. For example, if you have 100TiB of data and grow at 20TiB per year, you will have 160TiB at the end of year three. You would therefore expect to need around 320TiB peak storage on FlashBlade//S.

Be aware that this is a simplistic estimate. There are several factors that affect consumption, such as change rate, data reduction ratios, and full backup scheduling, so the exact amount of storage you will need can vary widely. For the example above, peak three-year consumption could be as low as 180TiB or as high as 470TiB as those factors change. You should consult with your Pure Storage and Commvault sales teams to get an accurate estimate for your own environment.

To optimize capacity usage with layered vaulting, you should configure the vaulting interval to start just before your full backups run. Due to the way data pruning works, the solution will use more storage the more time there is between sealing the vault and the next baseline backup. For example, if you run full backups starting every Friday evening, you will get the lowest capacity utilization if you seal your vaults during the day on Fridays.

Estimate Deduplication Database Requirements

The vaulting process will retain deduplication databases (DDBs) until all their references are stale. You will need enough storage to accommodate at least three DDBs to ensure you don't run into issues. If you use partitioned DDBs, each partition will need enough storage available.

Configuring Commvault for Object SafeMode

Follow FlashBlade//S Best Practices

Follow the best practices for using FlashBlade//S object storage with Commvault. Object SafeMode does not require any deviations, but there are several additional required steps and recommendations contained in this section.

Disable Micro Pruning

To avoid issues with data pruning, you must disable Commvault's micro pruning feature for any object buckets on FlashBlade//S arrays with Object SafeMode enabled. When micro pruning is enabled, Commvault can refresh some of its non-data objects after Object SafeMode retention expires, but before the objects are due to be deleted. When Commvault later tries to delete these objects, Object SafeMode will prevent the deletion, and these objects will prevent full cleanup of the vault. Over time these stale non-data objects can consume a significant amount of storage. Disabling micro pruning changes the behavior so the objects are never refreshed.

Micro pruning is configured using the CommCell Console, at the bucket or mount path. To disable micro pruning:

1. Expand Storage Resources, then Libraries. Expand the library for the FlashBlade//S. For each mount path, right-click the mount path and select Properties. In the Properties dialog box, select the Allocation Policy tab.
2. In the lowest section (Figure 6), clear the **Enable Micro Pruning** checkbox. Click the OK button to commit the change and click the OK button on the warning dialog that appears.

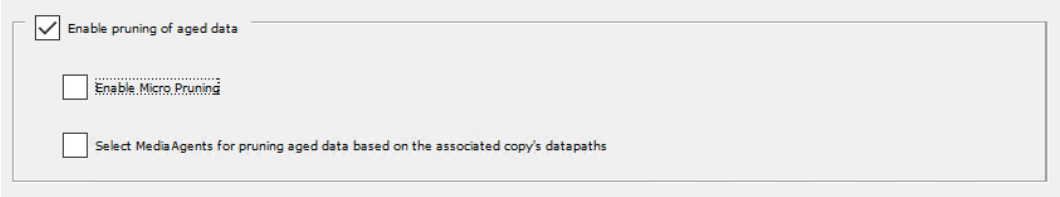

Figure 6. Disabling micro pruning

Rotate FlashBlade//S Object Storage Access Keys

You should regularly rotate access keys for FlashBlade//S object storage—creating a new key and deleting the old one—to minimize the risk of key compromise. The credential manager in Commvault makes the rotation process simple. To rotate keys, first create a new key pair on the FlashBlade//S. Access the Object Store view, then navigate to the account that contains the Commvault bucket. Click the user that has the key you want to rotate. Click the context menu button for the **Access Keys** tile, then select **Create access key** from the menu. A dialog will appear with the details of the new key (Figure 7).

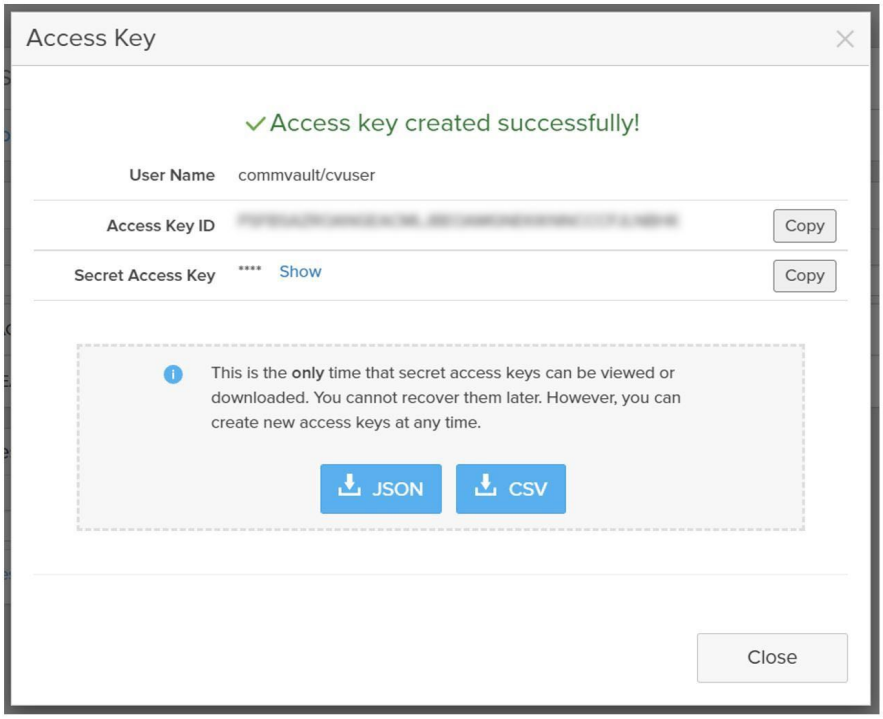

Figure 7. FlashBlade//S access key pair creation

Leave this page open and, in a separate browser window or tab, access the **Credential manager** view in Commvault Command Center. Click the stored credential for the FlashBlade//S bucket to open the **Edit credential** form (Figure 8). Replace the **Access key ID** and **Secret access key** fields with the newly generated key values, then click the **Save** button. You may export the keys for future reference; however, copying the key values between consoles using the **Copy** buttons will prevent an attacker from compromising the stored file. Running the consoles side by side lets you copy the keys in seconds.

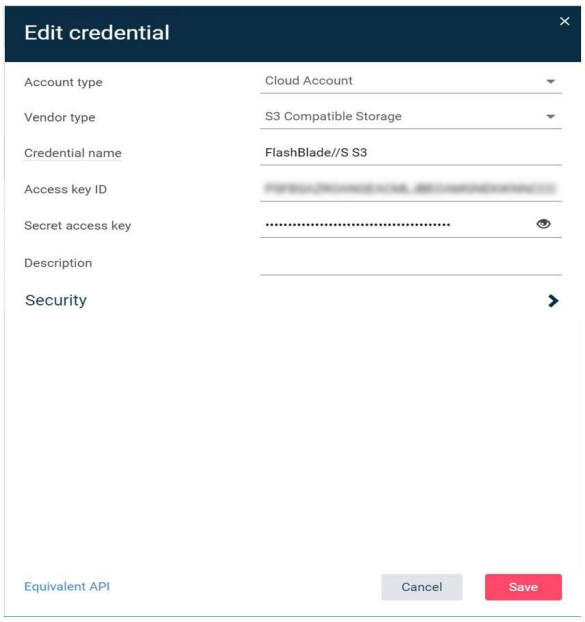

Figure 8. Updating access keys in Commvault Command Center

Once the key has been updated in Commvault, delete the old key from the FlashBlade//S to prevent compromise. In the FlashBlade//S UI, Click the **Close** button to clear the dialog box. In the **Access Keys** tile, click the context menu for the old key, then select **Delete** (Figure 9). When prompted to confirm deletion, click the **Delete** button.

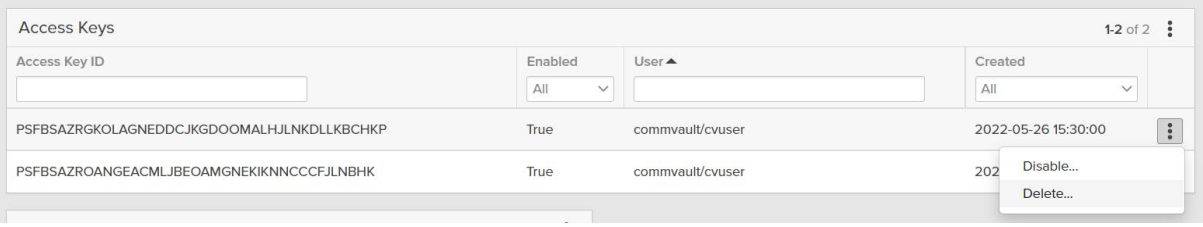

Figure 9. Deleting old access key

Avoid Storing Access Keys

Exporting access keys, especially secret keys, to store them in a file may seem like a reasonable step given the size and complexity of the key values. However, this creates a vector for an attacker to gain access to and alter or delete your backup data without your knowledge. Commvault stores the access keys in an encrypted form and doesn't ever display the secret key. An attacker would have to gain direct access to the CommServe database and obtain and decrypt the secret key to compromise the backup storage.

Since it is simple to generate new keys, it is better to generate a separate key if you need to do any direct access testing, then delete the key when testing is complete.

Set Appropriate Retention on Primary Copy Data

Retention on the Primary copy of your server backup plan or storage policy should follow the guidelines in Design Layered Vaulting Around Immutability SLA. Figure 10 shows an illustration of copy retention for a server backup plan with a 14-day vaulting interval and 28-day Object SafeMode retention period.

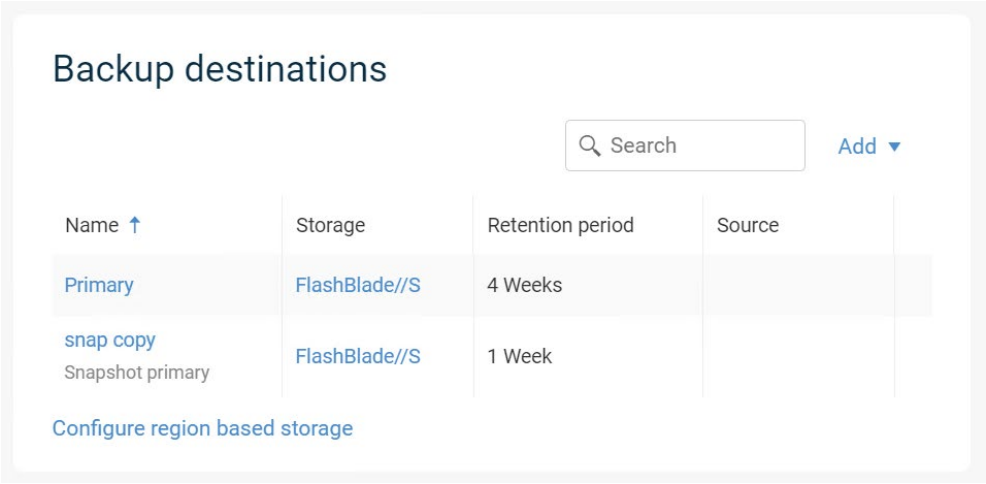

Figure 10. Primary copy retention in server plan

Configure Non-deduplicated Policy for Index and DDB Backups

Index and DDB backups related to FlashBlade//S will default to using the same server backup plan as the client data. However, Commvault manages their retention independently from the backup plans. When combined with periodic DDB sealing and Object SafeMode immutability, these backups can place dependencies on sealed DDBs that will make Commvault keep client backups longer than expected. This is especially true with immutability windows shorter than 21 days. To avoid these issues,

create a separate non-deduplicated storage pool and a storage policy specifically for index and DDB backups, then associate the index and DDB backup subclients to the new policy.

To create a non-deduplicated storage pool:

Create a cloud storage pool following the same procedure as in "Configure a Single Object Bucket" in Configuring Commvault with FlashBlade: Best Practices, but instead of adding DDB partitions, disable the **Use deduplication** option (Figure 11). Use the same bucket name and credentials as the deduplicated storage pool.

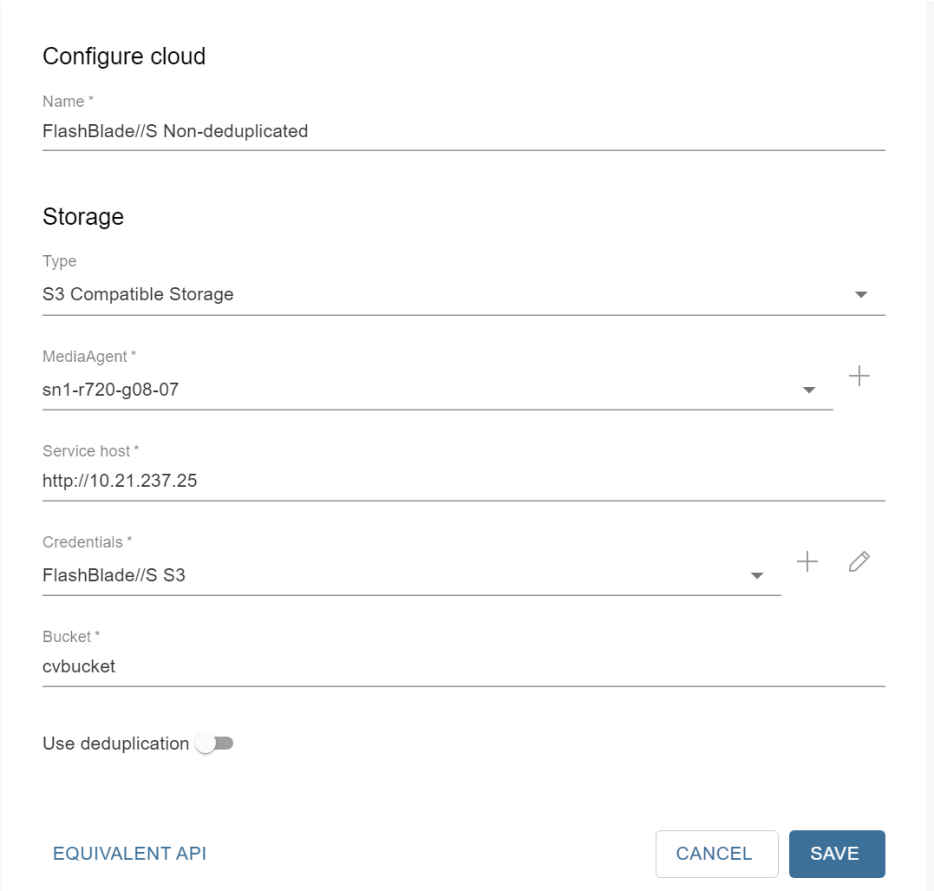

Figure 11. Adding a non-deduplicated cloud storage pool

Share the new storage pool to the same MediaAgents as the deduplicated pool, following the same procedure as in "Share the Bucket Across MediaAgents" in Configuring Commvault with FlashBlade: Best Practices.

To create a storage policy from the pool:

In the CommCell Console, expand **Policies**. Right-click **Storage Policies**, then click **New Storage Policy**. Complete the wizard as follows:

1. Select the **Data Protection and Archiving** option, then click the **Next** button.
2. Enter a name for the storage policy in the **Storage Policy Name** field, then click the **Next** button. Do not enable any of the checkboxes.
3. From the **Storage Pool** dropdown, select the non-deduplicated pool you created (Figure 12), then click the **Next** button.

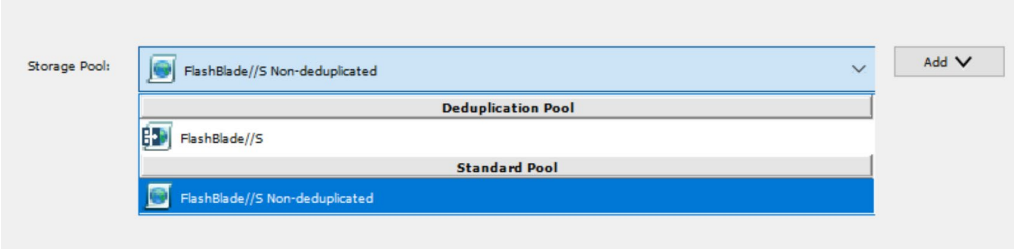

Figure 12. Storage pool selection

4. Set the storage policy retention to be longer than your Object SafeMode retention. If your Object SafeMode retention period is shorter than 30 days, accept the default primary retention setting of 30 days and 1 cycle (Figure 13). Click the **Next** button to continue.

Figure 13. Default data retention

5. Click the **Finish** button to create the storage policy.

To reassociate the index and DDB backup subclients for each FlashBlade//S server backup plan or storage policy:

1. In the CommCell Console, expand Policies, then click **Storage Policies**. In the right-hand pane, locate the storage policy associated with the server backup plan. Right-click the policy, then click **Properties**.
2. Select the **Associated Subclients** tab.
3. In the client list, select the index and DDB backup subclients, then click the **Re-Associate** button. You may need to resize the window to see the subclient names. In the Re-Associate Subclient(s) dialog box, select the new storage policy, then click the **OK** button (Figure 14).

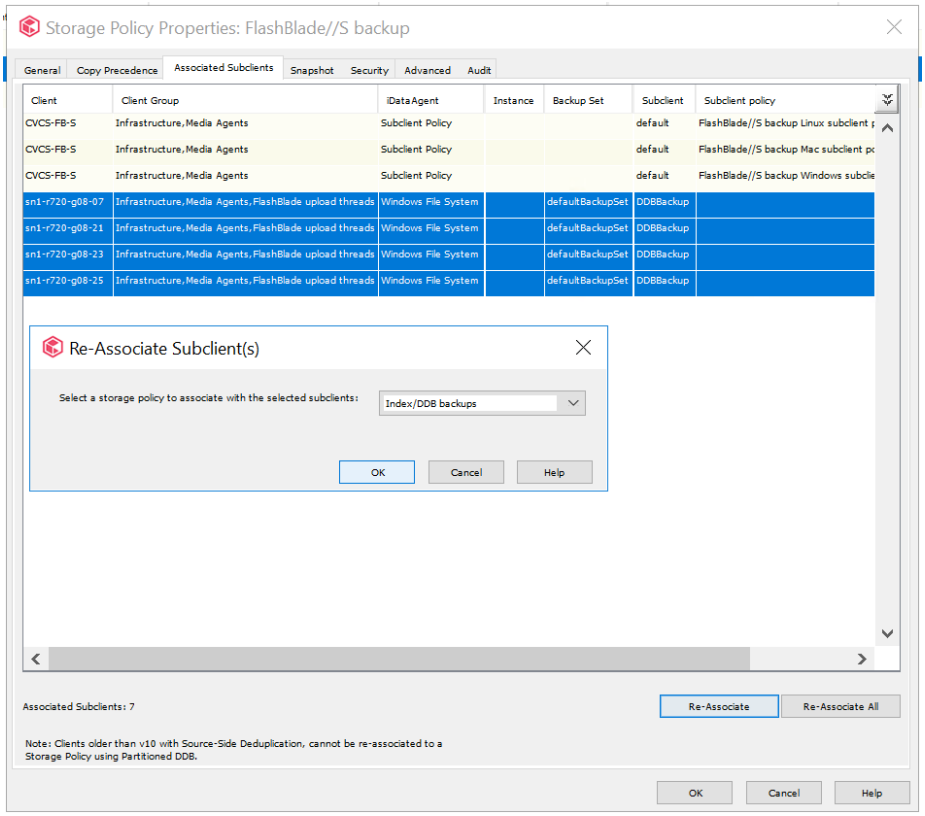

Figure 14. Reassociating subclients

4. Click the **OK** button to complete the association change. Subsequent backups will not be tied to the DDB and will not affect pruning of client data.

   IMPORTANT: If you create new server backup plans, storage policies, or storage pools using FlashBlade//S as a target, you must associate any new index or DDB subclients to the non-deduplicated storage policy.

Configure Commvault Vaulting Interval

For Object SafeMode to provide the desired immutability, you must configure Commvault to regularly seal the data vault by creating a new DDB on a regular interval. DDB settings are managed in the CommCell Console interface. In the CommCell Browser pane, expand Storage Resources, then expand Deduplication Engines. Right-click the appropriate DDB, then select Properties. In the dialog that opens, select the Deduplication tab, then the Settings tab on that properties page. Enable the first Create new DDB every checkbox, then set the desired number of days for the vaulting interval (Figure 15). Click the **OK** button to commit the change.

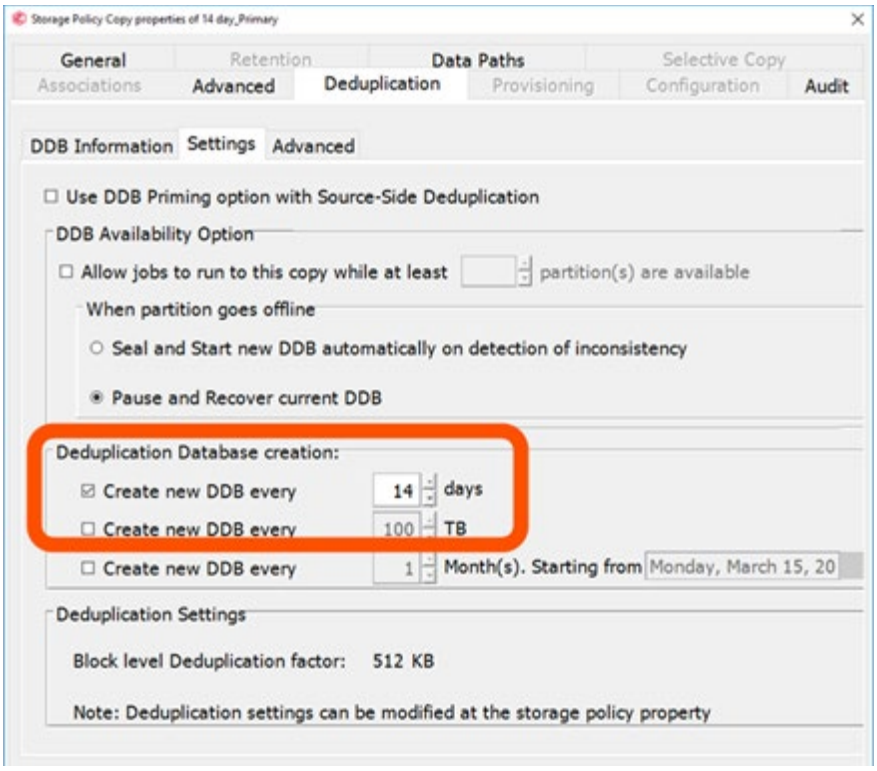

Figure 15. Setting Commvault vaulting interval

Seal DDB

After you disable micro pruning on the bucket and configure the vaulting interval on the DDB, you must seal any active DDBs associated with FlashBlade//S. This stops the micro pruning behavior on new data and sets a baseline for the automatic DDB sealing cycle. You should seal the DDBs 6-12 hours before your weekly full backups run to optimize capacity utilization.

To seal a DDB:

1. In the CommCell Console, expand **Storage Resources**, then **Deduplication Engines**. Locate the engine for the FlashBlade//S bucket and expand it.
2. For each database under the deduplication engine, right-click the database, then click **Seal Deduplication Database** (Figure 16).

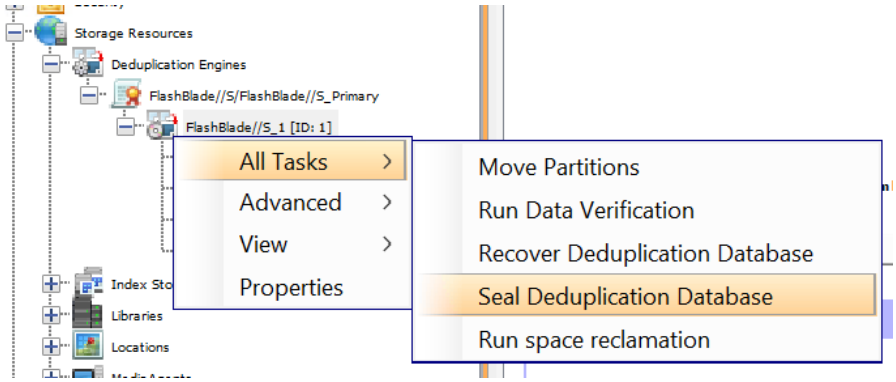

Figure 16. Sealing a DDB

3. If backups have already run using this DDB, you will be prompted to confirm sealing the database. On the confirmation dialog box, click the **Yes** button (Figure 16). Note: You may see a different confirmation message than Figure 17 shows.

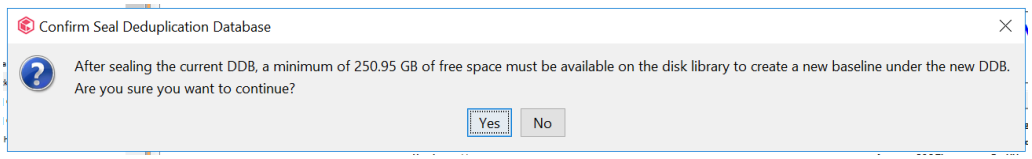

Figure 17. DDB sealing confirmation

Enable Object SafeMode

Once the Commvault settings are in place, you can contact Pure Support to enable Object SafeMode. Remember to have retention set to twice the vaulting interval, so if Commvault seals the vault every 14 days, Object SafeMode retention should be set to 28 days.

Implementing Object SafeMode in Existing FlashBlade//S Environments

If you are already using FlashBlade//S object storage as a Commvault backup target and want to add ransomware mitigation with Object SafeMode, you can follow the steps in this section. Make sure to contact your Pure account team before starting so they can assist along the way.

Calculate System Capacity Requirements and Vaulting Layers

Under-provisioning storage when using Object SafeMode can create a severe capacity risk. It is crucial that you properly size your FlashBlade//S before you make any configuration changes. Your Pure account team can assist you in generating an accurate projection based on current data size, daily change rate, and annual growth.

Follow the guidance in Design Layered Vaulting Around Immutability SLA to determine the intervals for your vaulting layers.

Upgrade to Minimum Versions

Enabling Object SafeMode with existing buckets requires a minimum version of Purity//FB 3.3.3. All FlashBlade//S systems ship with at least version 4.0.0; first-generation FlashBlade systems on release 3.3.2 or below must be upgraded.

We strongly recommend upgrading Commvault to version 2022E.

Suspend Backup Operations

Changes to certain policies can only be made when no backups are running. Disabling backups prevents these steps from failing, and it helps set a clear baseline for data vaulting. You can disable backups through Command Center or the CommCell Console.

To use Command Center to disable backups, use the left-hand navigation to access the Manage/CommCell page. In the **Activity control** tile (Figure 18), disable the **Data backup** slider.

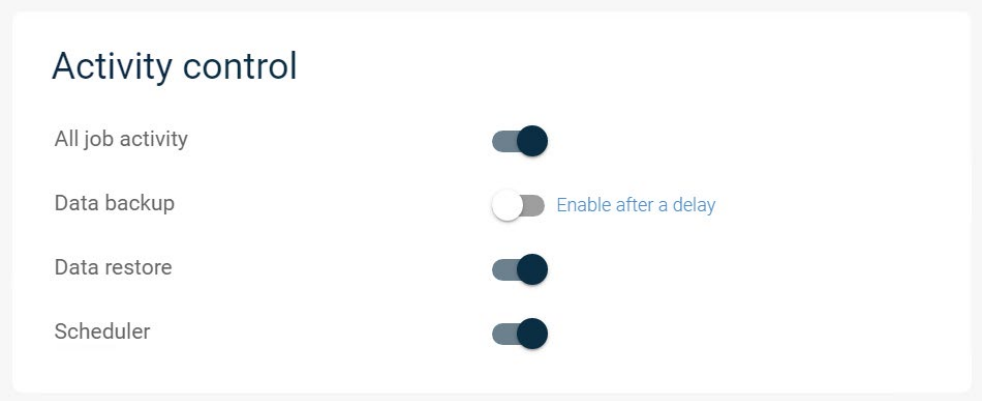

Figure 18. Disabling backups through Command Center

Update Retention Settings on Server Backup Plans and Storage Policies

For each server backup plan writing data to FlashBlade//S, you must change the retention for all of them to match what you calculated with your vaulting layers. If you have multiple data copies in your plans or policies, you only need to change the FlashBlade//S copy. If you wish to have longer or shorter retention than you calculated, please discuss the impact with your Pure account team before making any changes.

Configure Non-deduplicated Policy for Index and DDB Backups

Follow the steps in Configure Non-deduplicated Policy for Index and DDB Backups to create a non-deduplicated storage policy to hold your index and DDB backups without creating dependencies on the deduplicated vaults.

Disable Micro Pruning on FlashBlade//S Mount Paths

Follow the steps in Disable Micro Pruning to ensure data pruning happens on the expected schedule.

Configure DDBs to Automatically Seal

Follow the steps in Configure Commvault Vaulting Interval to set the frequency for sealing DDBs, which must match the immutability interval you defined with the vaulting layers.

Seal All DDBs Associated with FlashBlade//S

Follow the steps in Seal DDB to seal all the DDBs associated with existing backups to FlashBlade//S. This sets the starting point for the vaulting interval and ensures micro pruning is properly disabled for subsequent backups.

IMPORTANT: To optimize capacity, seal the DDBs within 12 hours before most of your full backups run.

Mark Sealed DDB Partitions for Recovery

Even after sealing the DDBs, Commvault will still attempt to use micro pruning for existing backup data. To prevent capacity issues this may cause, you must mark all the partitions of the sealed DDBs for recovery using the CommCell Console:

1. In the CommCell Browser pane, expand **Storage Resources**, then **Storage Pools**. Locate and expand the pool associated with the FlashBlade//S. Under that pool, expand **Deduplication Engines**, then the engine itself. Expand the item named **Sealed** to display the DDBs.

2. For each sealed DDB, expand the database to show the partitions. Right-click each partition, then click **Mark for Recovery**.

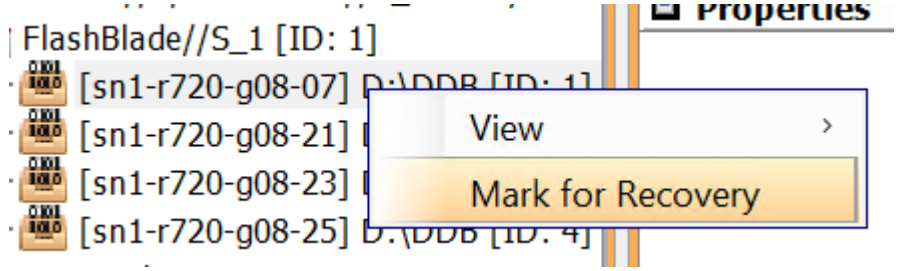

Figure 19. Marking a DDB partition for recovery

3. In the confirmation dialog box, click the **Yes** button. Since the DDB is sealed, Commvault will not take it or the active DDB offline or run a reconstruction job.

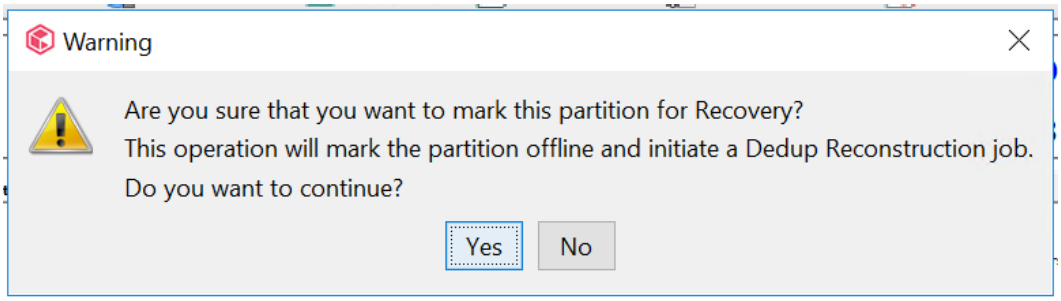

Figure 20. DDB recovery confirmation dialog box

Resume Backup Operations

When the Commvault vaulting layers have all been configured, you can enable backups again. Object SafeMode will apply retroactively to any existing data in the FlashBlade//S bucket.

To use Command Center to disable backups, use the left-hand navigation to access the Manage/CommCell page. In the **Activity control** tile (Figure 21), disable the **Data backup** slider.

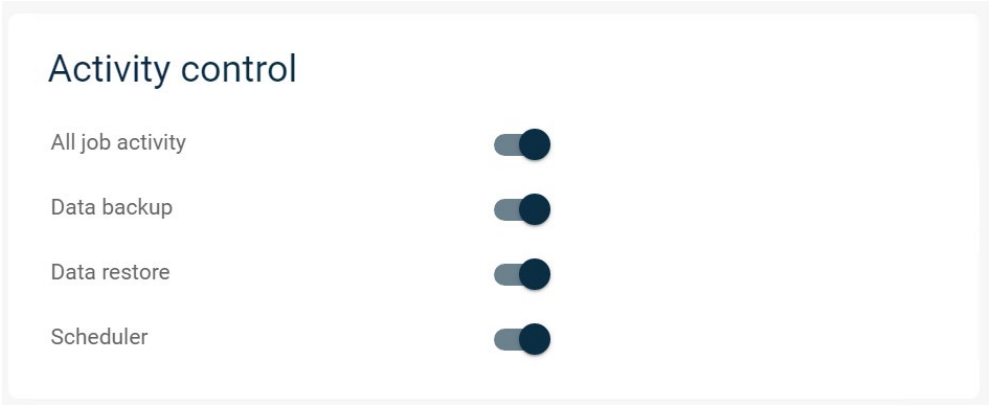

Figure 21. Disabling backups through Command Center

Work with Pure Support to Enable Object SafeMode

Once the Commvault settings are in place, you can contact Pure Support to enable Object SafeMode. Remember to have retention set to twice the vaulting interval, so if Commvault seals the vault every 14 days, Object SafeMode retention should be set to 28 days.

CommServe DR backup

CommServe DR backups are critical to recovery if an attacker compromises the CommServe. Placing them on a FlashBlade//S SMB file share and protecting them with SafeMode Snapshots ensures you can quickly recover your Commvault environment if necessary. If you have a second FlashBlade//S, replicating the DR backups gives you an added rapid recovery source in case of a site loss. This section details how to configure FlashBlade//S and Commvault for optimal DR backup protection.

Use a Dedicated Service Account

Using a dedicated service account ensures that the DR backups can't be accessed and therefore altered or deleted by any other account. The service account should not be used for any other purpose or allowed local login to any systems. If you have a password vault product, use it to store the password.

> IMPORTANT: If you are using FlashBlade//S SMB in AD RFC2307 mode, the service account must have values set for the uidNumber and gidNumber attributes in Active Directory for authentication and ACLs to work properly. If you are using Native mode, you do not need to set these attributes.

Create File System with SMB Export Policy

As shown in Figure 22, create the DR backup file system with only SMB enabled.

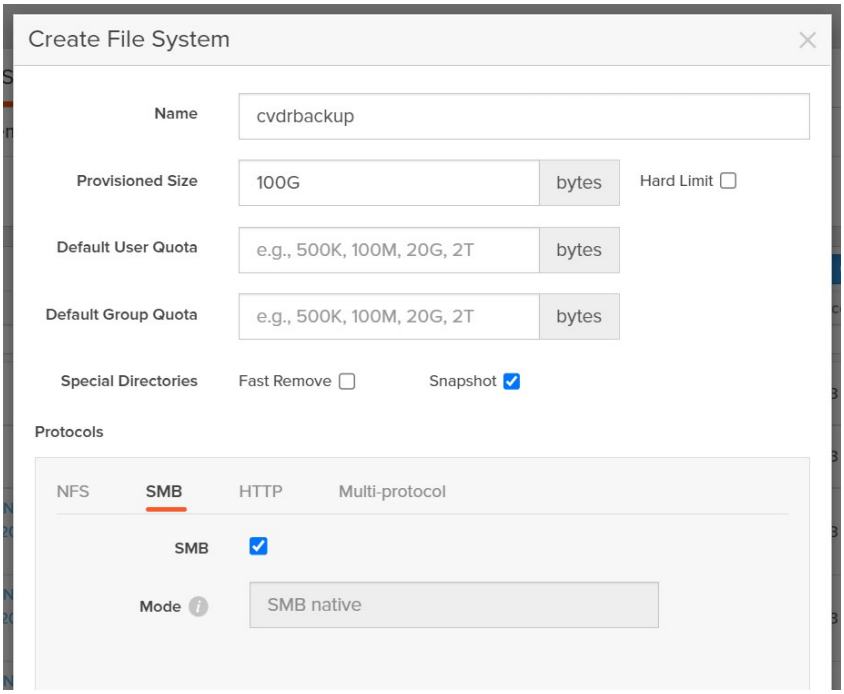

Figure 22. Creating DR backup file system with SMB export enabled

Restrict Access Using ACLs

The DR backup share ACL needs to restrict access so that only the service account can write to and manage the file system. Grant full control access for the service account to all files and directories in the share.

The CommServe DR recovery uses a restore within Microsoft SQL Server that runs as the SQL Server service account. Using the Commvault recommended configuration, this process will access the SMB share as the CommServe computer account. For DR recovery to work, the standby CommServe computer account also needs access. The ACL should grant only read access. For DR recovery on the production CommServe, the production CommServe computer account will also need read access.

For easier permissioning, create a group in Active Directory and add all the CommServe computer accounts to the group. Grant the group read access to the DR backup SMB share. Figure 23 shows the full ACL.

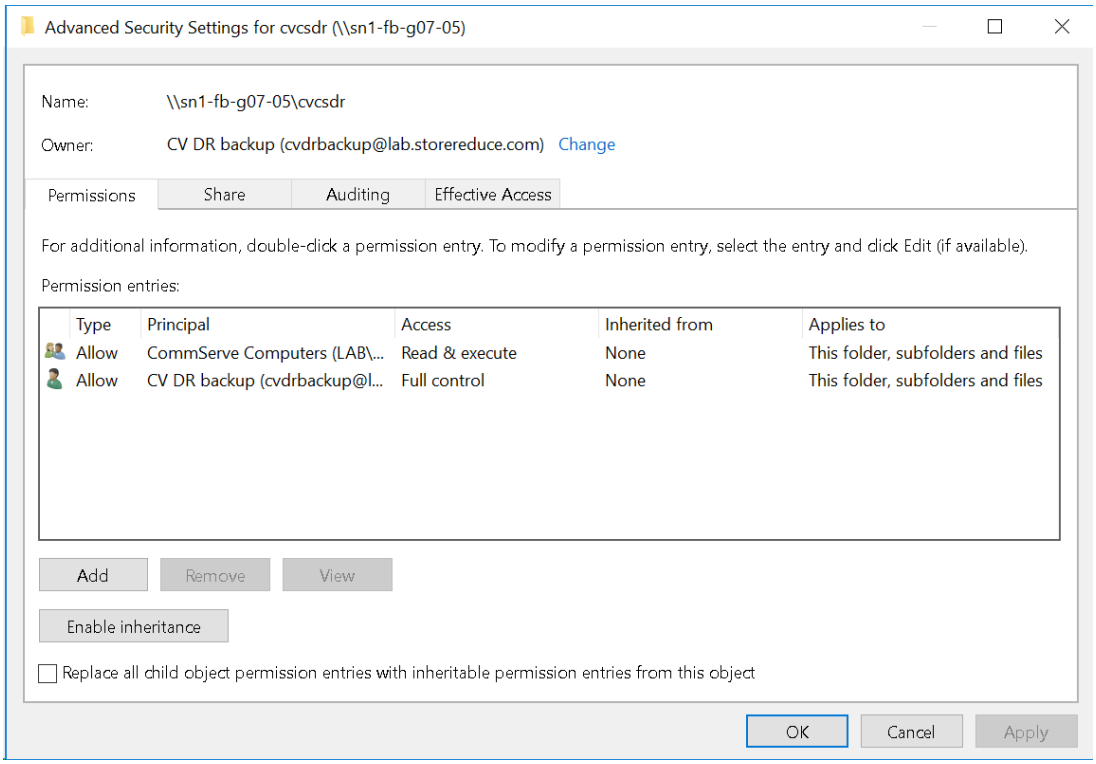

Figure 23. DR Backup SMB share ACL

Consolidate DR Backups for Multiple CommServe Systems

Every CommServe in an environment needs to run DR backups, including standby systems. Every CommServe can benefit from SafeMode snapshots if you consolidate the DR backups onto a single file system. Create a separate directory per CommServe to avoid conflicts between CommServe systems. All DR backups can use the same service account.

The ACL on the DR backup share needs to grant read access to every CommServe computer account in Active Directory to ensure recoverability.

Schedule DR Backups Close to the SafeMode Snapshot Schedule

To minimize the period where CommServe DR backups are not protected by SafeMode, schedule the DR backups to occur just before the snapshot policy schedule, making sure to allow enough time for the backup to complete. For example, if the SafeMode schedule runs at 10:00 a.m., and the backup completes in one minute, schedule DR backups for 9:55 a.m.

Use FlashBlade//S Replication to Provide Offsite Availability

While not detailed as part of this architecture, native replication between FlashBlade//S arrays coupled with SafeMode snapshots will provide an extra layer of defense for CommServe DR backups. Enabling replication with SafeMode snapshots can have broader implications, which you should discuss with your Pure Storage account team before implementing. Refer to FlashBlade//S documentation for more detail on enabling replication.

Upload Backups to FlashBlade//S Cloud Library

DR backups can be uploaded automatically to a configured cloud library, with longer retention than the first stage network share backup. Enabling this option is an easy way to get a longer-term copy of DR backups on FlashBlade//S Object Store.

To enable cloud library upload using Commvault Command Center, navigate to the **Manage/System** view, then select **Maintenance**. Click the **DR backup (Daily)** tile to fetch the settings, then click the **Edit** button (gear icon) to open the properties. As shown in Figure 24, enable the **Upload backup metadata to cloud library** option, then select the FlashBlade//S cloud storage from the **Cloud library** dropdown. Click the **Save** button to commit any changes.

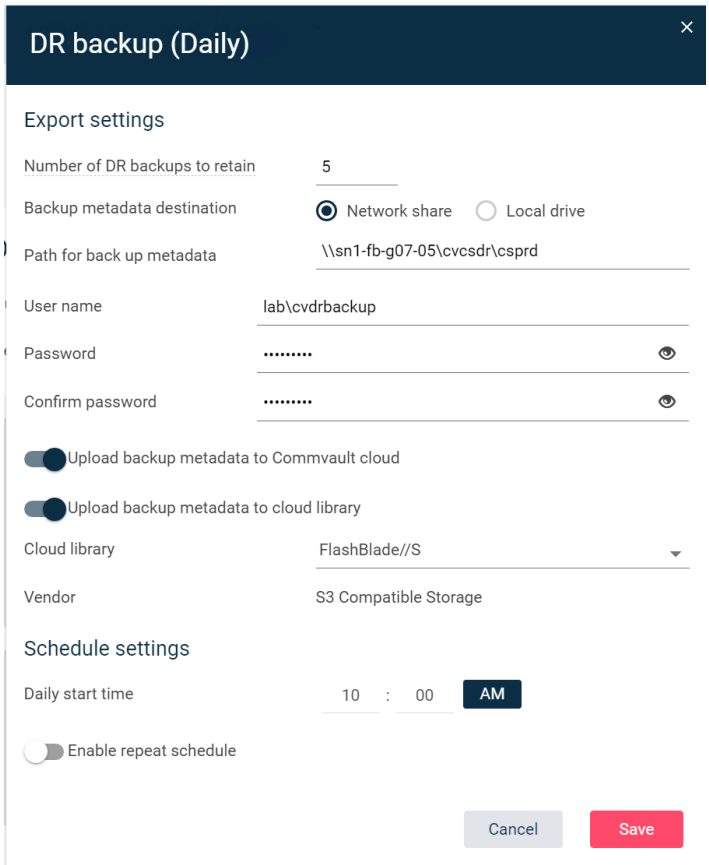

Figure 24. DR Backup configuration in Commvault Command Center

Upload Backups to Commvault Cloud

Commvault provides cloud storage for DR backups as part of a paid support agreement. This ensures an offsite copy is available in case of site loss or other situation that prevents using the local copies. This option should be enabled if allowed by your company policies.

Set Appropriate DR Backup Retention

By default, Commvault will keep five daily DR backups on the FlashBlade//S SMB share. SafeMode snapshots will extend that period based on the retention policy you define. For example, if the DR backup retention in Commvault is set to five, and the SafeMode snapshot retention policy keeps seven days, twelve days of DR backups will be available for recovery. Make sure to set these values appropriately for your needs.

Recovering from a Ransomware Event

Object SafeMode prevents ransomware, rogue administrators, or other data loss events from affecting your backup data, so you can focus on getting affected systems back online faster. You don't need to take any action on the FlashBlade//S since your immutable data remains available and uncompromised.

Clean Room Recovery

As part of the recovery, you should use a "clean room" approach to restore systems and data in an isolated space. You can then remove any malware before reintroducing the systems to the production environment. Pure Storage can help define what changes you need to make to make the FlashBlade//S accessible from the clean room.

Contact Pure Support

While you can begin restoring your primary systems right away, we recommend contacting Pure Storage Support, especially if you store production data on FlashBlade//S file systems or any other Pure Storage products. Support can be ready to assist with any issues you might encounter or changes you need to make to SafeMode settings.

Caveats

Please bear the following points in mind when working with Commvault, FlashBlade//S, and Object SafeMode:

- Synthetic full backups that run after the DDB is sealed will take longer to complete as the baseline is rebuilt. Depending on your environment, traditional full backups may be faster, but they will add load to your production systems. Other synthetic full backups will be faster.
- On the recommended Purity//FB releases, you cannot destroy buckets when Object SafeMode is enabled. Your authorized contact must work with Pure Support to enable the destroy operation for a specific bucket.
- Enabling Object SafeMode with existing buckets is only supported when no buckets have ever had object versioning enabled. If you have enabled versioning on a bucket and would like to enable Object SafeMode, please contact your Pure account team.
- Disabling and removing schedules from subclients will affect data aging for entire vault copies. To ensure Commvault can delete data on schedule, you must manually delete backups for retired subclients. If you want to archive the data from these subclients, use a separate storage pool for the archive copy.

- Delays in auxiliary copy can prevent DDBs from sealing on the expected schedule. Monitor aux copy jobs to ensure they are completing reliably.
- After enabling Object SafeMode in existing environments, you may see pruning failures for some older data in CVMA.log. These are because Commvault has been refreshing some of its internal non-data objects, so they will not have met the Object SafeMode retention age before Commvault tries to delete them. The errors will disappear over time and are not cause for alarm.

Additional Resources

- Pure Storage FlashBlade//S documentation
- Best Practices for Configuring Commvault with FlashBlade//S
- Commvault documentation

About the Author

Roy Child is a Senior Solution Architect with Pure Storage, responsible for defining data recovery solutions around various data protection applications. He is responsible for defining Pure Storage solutions and reference architectures for protecting and recovering primary workloads such as Oracle, SQL, and VMware. Roy has worked in and with the data protection industry for 20 years, from end user to IT architect with multiple backup and recovery products, followed by product management with Commvault. Roy joined Pure Storage in April 2019.

Pure Storage, Inc.
650 Castro Street, #400
Mountain View, CA 94041

PS2052-02 09/2022